

ELECTRONIC FILING

Peter M. Connolly
202 862 5989
peter.connolly@hklaw.com

February 27, 2009

Marlene H. Dortch
Secretary
Federal Communications Commission
445-12th Street, SW
Suite TW-A325
Washington, DC 20554

RE: **EB Docket No. 06-36**
Annual 47 C.F.R. § 64.2009(e) CPNI Certification for 2008
United States Cellular Corporation and affiliates

Dear Ms. Dortch:

Herewith transmitted, on behalf of United States Cellular Corporation and its affiliates, are its 2008 CPNI Certification and Accompanying Statement for filing in the above-referenced docket.

In the even there are any questions in connection with this filing, please communicate with the undersigned.

Very truly yours,


Peter M. Connolly

Enclosures

cc: Enforcement Bureau, FCC (2) via 1st class mail, US Postal Service
Best Copy and Printing, Inc. (1) via electronic mail

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008

Date filed: February 27, 2009

Name of company covered by this certification: United States Cellular Corporation and its affiliates listed in Attachment A

Form 499 Filer ID: See Attachment A

Name of signatory: Steven T. Campbell

Title of signatory: Executive Vice President - Finance, Chief Financial Officer and Treasurer


I, Steven T. Campbell, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 47 C.F.R. § 64.2001 et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission) against data brokers in the past year.

The company has reported a total of twenty incidents concerning the alleged unauthorized release of CPNI in the past year. Sixteen of these incidents were from complaints received from customers with the remaining four incidents being internally identified and reported. This small number of complaints is from a customer base of over six million customers. Of these reported alleged incidents, ten were related to instances of improper disclosure to individuals not authorized to receive the information, eight were related to improper access to online information by individuals not authorized to view the information, and two were related to instances of improper access by employees. Most of these incidents were related to domestic disputes and none of the incidents involved more than one customer account.

Signed



Steven T. Campbell
Executive Vice President – Finance, Chief Financial Officer and Treasurer
United States Cellular Corporation

Attachment A
Company Names and Filer ID

Filer ID	Company Name
802585	Illinois RSA No.3, Inc.
802586	USCOC of Illinois RSA No. 4, Inc.
802587	North Carolina RSA No. 9, Inc.
802608	California Rural Service Area 1, Inc.
802611	USCOC of Pennsylvania RSA # 10-B2, Inc.
802614	Hardy Cellular Telephone Company
802621	USCOC of New Hampshire RSA # 2, Inc.
802623	Vermont RSA No. 2-B2, Inc.
802626	Manchester-Nashua Cellular Telephone L.P.
802638	Davenport Cellular Telephone Company
802641	USCOC of Greater Iowa, Inc.
802644	Cedar Rapids Cellular Telephone, L.P.
802647	Bangor Cellular Telephone Company, L.P.
802653	USCOC of Greater Missouri, LLC
802655	Ohio State Cellular Phone Company, Inc. (for Roanoke)
802657	Ohio State Cellular Phone Company, Inc. (for Lynchburg)
802658	Charlottesville Cellular Partnership
802662	USCOC of Iowa RSA No. 1, Inc.
802665	USCOC of Greater Missouri, LLC
802668	USCOC of Illinois RSA No. 1, Inc.
802672	USCOC of Greater Missouri, LLC
802678	Ohio State Cellular Phone Company, Inc. (for NC 3)
802679	USCOC of Virginia RSA # 2, Inc.
802685	USCOC of Cumberland, Inc.
802687	USCOC of Iowa RSA No. 16, Inc.
802690	Ohio State Cellular Phone Company, Inc. (for Iowa 5)
802692	Kansas #15 LP
802695	Iowa 13, Inc.
802704	La Crosse Cellular Telephone Company, Inc.
802716	Tennessee RSA No. 3 Limited Partnership
802722	Tennessee RSA No. 4 Sub 2, Inc.
802731	USCOC of South Carolina RSA # 4, Inc.
802737	Yakima MSA Limited Partnership
802740	Lewiston CellTelCo Partnership
802743	Dubuque Cellular Telephone, L.P.
802746	Farmers Cellular Telephone Company, Inc.
802749	Iowa RSA No. 9 Limited Partnership
802752	Waterloo Cedar Falls CellTelCo
802755	Iowa RSA No. 12 Limited Partnership
802758	United States Cellular Operating Company of Medford
802761	McDaniel Cellular Telephone Company
802764	USCOC of Washington 4, Inc.
802767	Oregon RSA # 2, Inc.
802779	Western Sub-RSA Limited Partnership
802785	USCOC of Oregon RSA # 5, Inc.
802794	USCOC of Greater Missouri, LLC
802797	USCOC of Greater Missouri, LLC
802809	United States Cellular Telephone of Greater Tulsa L.L.C.
802818	North Carolina RSA No. 4, Inc.
802821	Indiana RSA No. 5 Limited Partnership

Attachment A
Company Names and Filer ID

802824	Indiana RSA No. 4 Limited Partnership
802833	United States Cellular Telephone Co. (Greater Knoxville), L.P.
802849	Texahoma Cellular L.P.
802851	N H # 1 Rural Cellular, Inc.
802860	Maine RSA No. 1, Inc.
802863	USCOC of Oklahoma RSA # 10, Inc.
802866	USCOC of North Carolina RSA # 7, Inc.
802869	Virginia RSA # 7, Inc.
802875	North Carolina RSA No. 6, Inc.
802878	Virginia RSA # 4, Inc.
807699	USCOC of Virginia RSA # 3, Inc.
817222	Green Bay Cell Tel Co.
817226	Madison Cellular Telephone Company
817228	USCOC of Rockford, Inc.
817230	Kenosha Cellular Telephone, L.P.
817232	Racine Cellular Telephone Company
818126	Jacksonville Cellular Telephone Co.
818128	Wilmington Cellular Telephone Co.
820095	USCOC of Greater Missouri, LLC
821502	USCOC of Greater Missouri, LLC
821504	USCOC of Richland, Inc.
821506	Maine RSA # 4, Inc.
821508	United States Cellular Operating Company
821600	Y-12 WIRELESS, L.P.
822062	BMG GROUP, L.L.C
822442	United States Cellular Operating Company of Chicago, LLC
823622	USCOC of Rochester, Inc
823624	USCOC of St. Joseph, Inc
825693	USCOC of KS/NE Inc.

2008 Statement of CPNI Compliance Procedures

United States Cellular Corporation on behalf of its CMRS operating affiliates (collectively "U.S. Cellular" or the "Company") has established operating procedures intended to ensure compliance with the requirements of Section 222 of the Telecommunications Act of 1996, as amended, and with the implementing rules adopted by the Federal Communications Commission at 47 C.F.R. Part 64, Subpart U ("CPNI Rules"). Unless otherwise stated, this statement reflects the operating procedures in place as of December 31, 2008.

Responsibility for the overall compliance of the Company with the CPNI requirements lies with the Director of Customer and Data Privacy who reports to the Vice President, Legal and Regulatory Affairs. Among other things, the Director of Customer and Data Privacy is required to do a year end assessment of the status of U.S. Cellular's compliance efforts with the CPNI Rules and other privacy protection initiatives. This process requires that key managers whose organizational day to day duties are impacted by the CPNI Rules be interviewed and provide a statement that U.S. Cellular's practices and procedures concerning protection of customer information are being adhered to. This process involved 27 interviews and the execution of 14 compliance statements attesting to the fact that U.S. Cellular's operating procedures ensure compliance with the CPNI Rules.

U.S. Cellular has implemented the following procedures in order to protect the CPNI of our customers:

Permission Notice for use of CPNI by Agents and Affiliates:

Currently, U.S. Cellular exclusively provides CMRS services. Thus, every marketing interaction that it has with customers is exclusively "within category" as the FCC has defined that term and for which no explicit permission from customers is required to access and use a customer's CPNI. U.S. Cellular also has an Agent distribution channel for both in-bound and out-bound customer interactions and relationships with other affiliates who may from time to time have a need to access customer information for marketing telecommunication services to customers. With respect to the use of CPNI by Agents and Affiliates, U.S. Cellular obtains permission from customers using the FCC sanctioned Notice and Opt-Out method as follows:

- Postpay customers who receive a monthly bill by mail receive a CPNI Notice in the form of a bill insert included with the customer bill informing them about CPNI and their right to restrict its use, disclosure, or access. Prepay customers with a valid name and address receive a letter mailed to the address of record providing them with the same CPNI Notice. Copies of the CPNI Notice are posted on U.S. Cellular's website as well as made available upon request at its retail stores or through its call centers.

- Although not required by the CPNI rules, all mailed notices are in dual language (English and Spanish) and the contents of the Notice satisfy the substantive requirements of 47 C.F.R. 2008 (2)(c)(1) through (10).
- A campaign calendar is maintained and a campaign management system is used to generate campaigns for CPNI notices to existing customers no later than every 2 years.
- Customers are given a minimum of 33 days to respond to the CPNI Notice before they are considered to have provided implied consent to allow Agents to use, disclose, or access their CPNI for marketing purposes. The billing system maintains the CPNI status of a customer as either in their initial notification waiting period or opted out, or having provided implied consent. Agents have received specific written direction that they are not to access any CPNI from new customers for marketing purposes until the time period has passed for determining the customer's CPNI permission status.
- An Interactive Voice Response ("IVR") system with a dedicated toll-free number is available on a 24/7 basis (except for minimum downtime for required maintenance in off-hours) for customers to contact in order to opt-out. Customers also may visit a Company owned retail store or contact a Company owned call center to opt-out. Customer calls are automatically routed to a call center in the event that the IVR is unavailable. There is no additional cost to the customer to use any of these opt-out methods.
- A process is in place for the monitoring, reporting, and escalation of the IVR system's availability to support customer opt-out calls.

Approval for use of CPNI:

- Customer elections to opt-out from providing their consent to allow retail agents and third party call centers ("Agents") to use, disclose, or access their CPNI for marketing purposes remain in effect until a customer requests that such election be revoked.
- Records of customer opt-out elections are maintained in our customer information billing system for at least as long as the customer remains in active status.
- Customers' opt-out status is automatically updated daily in the campaign management system used by the internal U.S. Cellular marketing associates who prepare marketing campaigns. Agents of U.S. Cellular are instructed in writing that they should not contact customers that have not provided implied consent for marketing purposes in which CPNI is used. These customers are contacted only by U.S. Cellular's own internal telemarketing and sales associates.

General Safeguards for use of CPNI

- All Company and Agent associates are required to take CPNI training within their first 30 days of employment or prior to working in a front line position. Additional policy and procedures training is provided to front line associates.
- U.S. Cellular has an express disciplinary process in place to protect customer privacy and CPNI. While associates are subject to progressive disciplinary actions for failures to comply with the Company's policies pertaining to customer privacy and CPNI, a failure to authenticate a customer in accordance with the Company procedures for doing so or providing call or text message detail over the phone is subject to the most significant disciplinary action and is grounds for immediate termination. Agents of the Company are informed in writing of their obligations to protect customer privacy and CPNI and are subject to disciplinary actions including possible contract termination for non-compliance with the terms of their agreements.
- Company and Agent direct marketing and market research campaigns to existing customers using CPNI are documented, reviewed, and approved by a manager with supervisory authority. U.S. Cellular policy requires that the campaign records be stored for a minimum of one year.

Authentication

- Customers are authenticated when requesting CPNI over the phone by providing multiple elements of identification information. A pop up screen is provided on every inbound call to one of our call centers reminding associates that they must validate a customer before providing any information. The associate must close the pop-up screen in order to be able to proceed further and have access to any customer record. As described above, failure to validate a customer is subject to U.S. Cellular's disciplinary process regardless of whether the failure to validate resulted in the inappropriate use of CPNI.
- U.S. Cellular policy prohibits associates from using readily available biographical information ("RAB") or account information to prompt customers for their passwords.
- U.S. Cellular policy prohibits our associates from providing call detail over the phone even if the customer has been properly validated. U.S. Cellular policy requires that requests for call or text message detail from customer-initiated phone contacts by postpay customers be fulfilled by mailing the information to the address of record for the account.
- U.S. Cellular policy requires that our customers be authenticated by our associates and Agents with a valid photo ID before providing CPNI during an in-store contact at retail stores.

- Registration for an online account with access to billing information and CPNI requires a unique PIN in addition to account information and does not rely solely on RAB1 or account information. The PIN number is sent via a text message to the customer's handset for the account of record. Subsequent access to CPNI online by a customer requires a unique username and password which is established by the customer. Back up authentication methods for lost or forgotten passwords do not use RAB1 or account information. Customers that cannot provide the proper responses to back up authentication questions are required to go to a retail store and authenticate with a valid photo ID in order to reset their username or password.

Notification of account changes

- A text message is sent to the telephone number of record selected by the customer to notify them when an online account is established or when a password, username, email address, or response to backup authentication questions for the online account is changed.
- A letter is sent to the address of record when an authorized user, address of record, or password is created or changed over the phone on customer accounts. A letter also is sent for address changes requested through payment advices sent by the customer along with their bill payments.

Notice of unauthorized disclosure of CPNI

- An Incident Response process including a Privacy Incident Response Team ("PIRT") has been created to handle the identification, internal investigation, and reporting of events that may result in breaches of CPNI. The existence of PIRT has been communicated throughout U.S. Cellular with contact instructions in the event that an associate has reason to believe that a CPNI breach may have occurred.

Other measures to protect CPNI

- U.S. Cellular proactively alerts front line associates in sales channels and call centers when suspicious and unsuccessful pretexting attempts are identified. Alerts are given to the respective retail stores in the area or across call center departments to alert them to this activity.
- There are formalized processes that address the management of access to the centralized customer management system that stores CPNI. These processes address:
 - Requesting and approving access to applications that access CPNI, including administrative access. This process is partially automated.

- Periodic associate entitlement reviews for appropriate level of access, including administrative access. This includes protection against the accumulation of access rights during associate role transfers.
 - Removal of access rights for terminated associates. This process is partially automated.
 - Separate developer access procedures requiring higher level of approval that are routinely reviewed.
 - Periodic auditing of these processes.
- Vulnerability scans on externally-facing and internal U.S. Cellular systems are performed routinely. These activities attempt to discover vulnerabilities that may be exploited to compromise the security of the internal U.S. Cellular network and the customer data it contains.
- Layers of firewalls secure the network perimeter, DMZ, and internal systems. Firewalls restrict and filter connectivity to the systems that provide access to CPNI.
- Network intrusion detection systems and intrusion prevention systems are in place that monitor the network perimeter for network vulnerabilities or suspected compromises. Attack signatures are updated weekly on the network intrusion detection and prevention systems.
- Systems are patched to protect against known system vulnerabilities.
- Anti-virus software is installed on workstations to help protect against known viruses, worms, and Trojans.

All of the foregoing measures demonstrate that U.S. Cellular has established operating procedures that are adequate to ensure compliance with the FCC's CPNI Rules

In 2008, U.S. Cellular experienced periodic attempts by pretexters to gain access to CPNI or other customer personal information. Most documented instances of attempted unauthorized access to customer data experienced by U.S. Cellular appear to be related to domestic disputes. In other cases, pretexters attempted to get information (typically confirmation of a billing address) over the phone by posing as a Company associate claiming to be having problems accessing customer information from their alleged work locations. U.S. Cellular provided additional training and awareness to front line associates to address these specific pretexting attempts. An additional safeguard to thwart pretexters was recently implemented which requires associates to provide a "security word" as part of the authentication process when handling requests for customer account information from other associates. The computer generated "security word" changes frequently and must be provided to discuss customer account information.